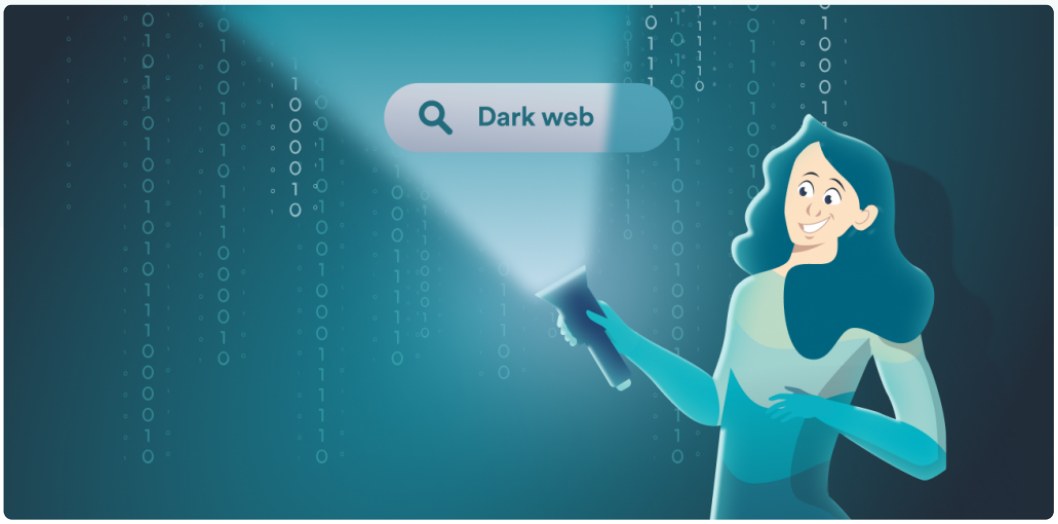
How to use Tor, and is it safe to access the dark web?

Aistė Jokšaitė in Cybersecurity, Internet Security
2022, March 9 · 10 min read



What happens when your need to be private online meets some of the wildest IT developments? Tor. However, the Tor network does not seem that easy to get into for the aspiring. That's why this article is here: you'll learn how to use the Tor Browser and maybe even where to go on the network.

Table of contents

1. What is Tor?
2. What is the dark web and how is it related to Tor?
3. How to use Tor
4. 6 tips on how to use the Tor browser safely
5. Where do I go on Tor?
6. Tor browser and the deep web
7. Is it illegal to use Tor?
8. Tor network: bring privacy to your everyday life
9. FAQ

What is Tor?

Tor is a network named after The Onion Router project that it's based on. It makes your browsing a lot more private by bundling your data into layers of

encryption (like an onion) and routing it through three nodes (volunteer-maintained systems that act as intermediaries for your internet traffic).

Any individual node only knows the previous and the next destination, so not even the entry node knows where you're going online – and the exit node has no idea who sent the data in the first place.

Other web browsers may offer private browsing and Incognito modes, but these modes do not hide your browsing history. Your internet provider will still know your browsing habits. Tor, however, can protect you from that.

What is the dark web and how is it related to Tor?

Although similar to the deep web in theory, the dark web can be a bit trickier. It is intentionally a lot more obfuscated and requires special effort to access. This can involve needing to enter a password before accessing a page which seems pretty normal. Something a little more out there is requiring you to use a certain browser to open these pages. That browser is Tor.

How to use the Tor browser to access the dark web?

As weird as it sounds to us, you could be turned away from a website because of your browser. The dark web is hard to access because it includes a lot of crime, but it also has dark web versions of mainstream news sites. This allows people in oppressive states to access undoctored news securely.

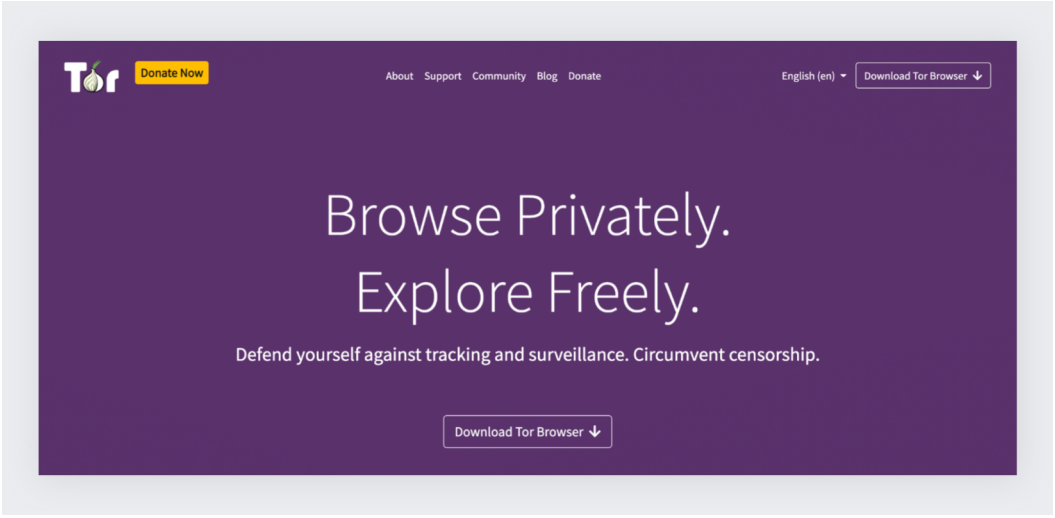
So you can not only use Tor to access the dark web, but you'll be encrypted as well. If you're okay with a slower connection, you could use Tor every day. And if it's not a compromise you're willing to make, just remember to use Tor every time you visit a website you don't want anyone in between to know you visited.

How to use Tor

Previously, using Tor was a bit annoying and required serious tech knowledge. Today, the Tor Browser project makes it as easy as pie. Here's how to use Tor:

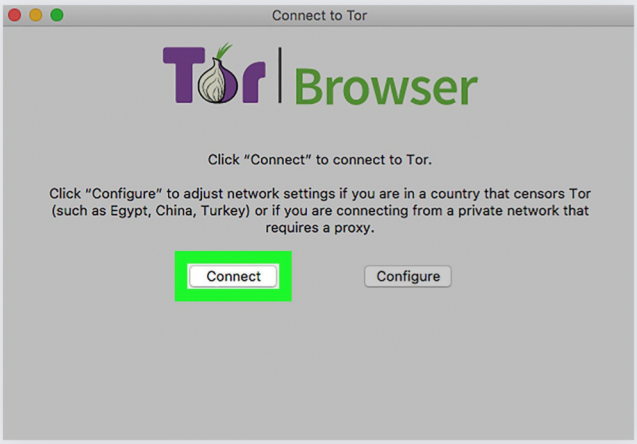
1. **Download and install the Tor Browser.**

Get the Tor Browser app (Windows, Mac, Linux, and Android are supported).



Once Tor installs, press **Finish,** and the browser will launch.

2. **Click Connect in the Tor Browser configuration window.**


Connect to Tor
Tor Browser
Click "Connect" to connect to Tor.
Click "Configure" to adjust network settings if you are in a country that censors Tor (such as Egypt, China, Turkey) or if you are connecting from a private network that requires a proxy.
Connect
Configure

Configure is for people who are using a proxy to access the internet.

3. Wait for the browser to connect to the node network.

The first time you do this, you will experience a delay. Tor can take several minutes to establish that first connection.

4. Start browsing the Tor network!

If you seek even more security, try using Tor together with a VPN connection.

Tor is based on the same code as Firefox, so the interface will look familiar. However, if you're not used to Firefox, no need to worry. It still functions similar to any other popular browser.

Now that you know the basics, let's delve deeper into the security of Tor.

Get an online security checklist — join our newsletter

Email address

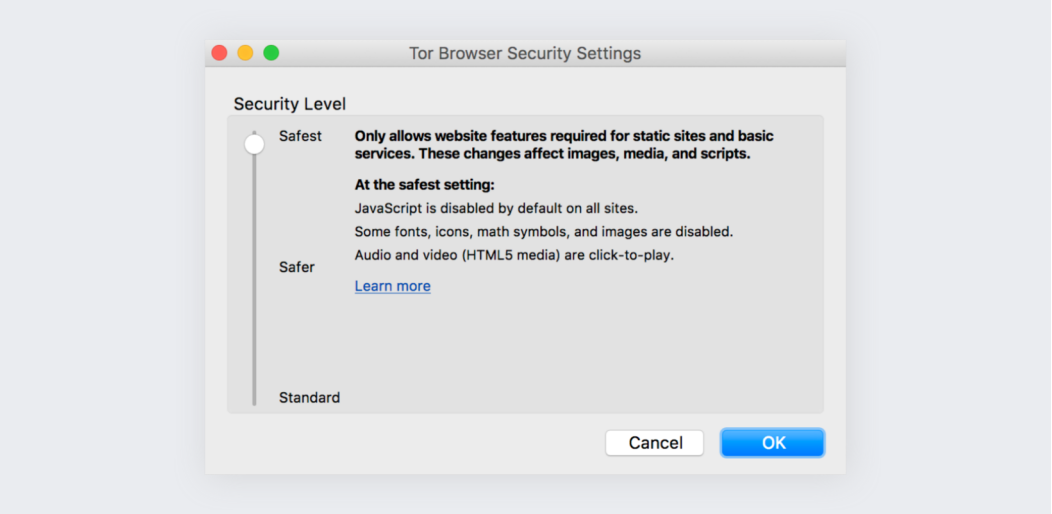
Join

6 tips on how to use the Tor browser safely

There is no single app that would secure you from every threat out there – you need to be aware of the best security practices yourself. Here's how you use the Tor Browser safely:

1. Set your security level

The Tor Browser comes with three layers of security. The settings are accessed by clicking the shield button next to the address bar and choosing **Advanced Security Settings**.


Tor Browser Security Settings
Security Level
Safest
Only allows website features required for static sites and basic services. These changes affect images, media, and scripts.
At the safest setting:
JavaScript is disabled by default on all sites.
Some fonts, icons, math symbols, and images are disabled.
Audio and video (HTML5 media) are click-to-play.
Safer
Learn more
Standard
Cancel
OK

- **Standard** is no different from operating any other browser.
- **Safer** *(recommended)* disables JavaScript on insecure websites, blocks some math symbols and fonts, and prevents most audio and video from playing by default. This can mess with the functionality of some sites.
- **Safest** cranks that up to 11, and only very basic websites work unimpeded. For example, Wikipedia users will not notice any differences; Buzzfeed is usable, Imgur isn't.

2. Check the other security settings

By default, the Tor Browser uses permanent private browsing mode. This means that history and website cookies get deleted every time you close the Tor Browser. When you start it up, it's like using a new browser. If you don't like this sort of thing, you can loosen the rules a little in the settings section.

3. Change your browsing habits

Did you know that Google tracks you? Even Tor can't protect you if you use search engines that track your activity.

So there's no sense in using the Tor Browser if you're just going to give away your data again. You should use search engines that don't track you, like DuckDuckGo (it's the default one on the Tor Browser) or Surfshark's Clean Web service.

4. Try new circuits and identities

Like VPNs, Tor hides your real IP and makes your location private. The collection of nodes the Tor Browser uses to connect you to your online destination is called "a circuit." If the website is working slowly or you want a new IP, click the shadowed window next to the website address. Here, you can request a new circuit – this will also reload the website.

A more powerful version of this is "new identity." This will close all windows and tabs and restart the Tor Browser itself. If you're on private browsing, it will be like starting up a new browser with a fresh new IP.

5. Use Tor over a VPN

There are three reasons why you'd want to use a VPN together with the Tor browser:

1. VPN encryption hides what you're doing online – including using the Tor Browser, as some ISPs and governments are suspicious of it.
2. A VPN hides your IP in case the entry node is compromised.
3. The Tor Project does not recommend using advertisement blocking extensions on the grounds of privacy (we're starting to see a pattern), but Surfshark VPN blocks many of the ads at the source.

You're using the Tor Browser because you want to be private online – and using a VPN compensates for some of Tor's weaknesses.

Surfshark does not encourage using a VPN in any way that would potentially violate the Terms of Service of other service providers.

6. Make sure your security measures are up to date

If you're going to use the Tor Browser to access deep web sites, you better make sure that you're as protected as possible. This means always updating your device's OS, having a working firewall, and a reliable antivirus system.

Where do I go on Tor?

Navigating the Tor network isn't easy as search engines do not index *.onion* sites. Therefore, you need to use sites like the Hidden Wiki to find out the specific web addresses.

Incidentally, we have an article on the best .onion sites for amateur Tor users.

Just keep in mind that these are sites from the deep and dark web and often require a bit more effort to access.

Tor browser and the deep web

What is the deep web?

“Deep web” is technically a term used to describe parts of the internet not indexed by search engines and thus not ordinarily reachable via them.

How to use the Tor browser to access the deep web?

Once you have the Tor Browser running, you can access a site on the deep web by simply entering the website address. The trouble is finding those addresses. After all, search engines don’t work for the deep web.

Note: some of those websites are hard to find because they’re dealing with illegal activities. Always be on alert.

Is it illegal to use Tor?

No, it’s not illegal to use Tor or the Tor Browser. However, doing illegal stuff over Tor is still, well, illegal.

Tor is popular with people taking part in shady activities (as well as whistleblowers and journalists). Therefore, the government may be interested in their users. There have already been cases in the past of, say, NSA looking into Tor users. Which is why you shouldn’t use Tor for illegal activities.

Tor network: bring privacy to your everyday life

Once you’ve learned how to use it, Tor isn’t as intimidating as it can seem at first. Sure, it involves a few extra steps that you would avoid with a normal web browser, but it’s worth it for your privacy. Of course, the Tor network cannot keep you completely safe, which is why we recommend using a VPN as well.

Get Surfshark VPN for the Tor Browser!

Try it with a 30-day money-back guarantee

Get Surfshark

FAQ

Can you be tracked on Tor?

In theory, being tracked over Tor is possible but it's not easy. Tor hides your real IP and your browser activity from your ISP by changing your circuit – the network nodes used to reroute your data – every ten minutes. However, the nodes are provided by volunteers. This means that government entities may control some nodes themselves.

Can I use Tor for P2P/streaming?

Written by

Aistė Jokšaitė

Searching for understandable synonyms for techie words.

Rate and share this article

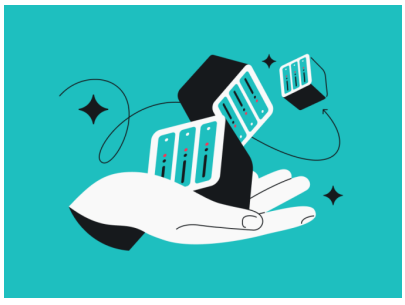
4.4/5

Hand picked related articles

What does private browsing do and what it doesn't do

Martynas Klimas in Internet Security

2023, November 30 · 12 min read



Proxy server: what is it, and do you need one?

Martynas Klimas in Cybersecurity, Internet Security

2023, November 22 · 19 min read

Does Incognito mode hide your IP address? No, here's why

Kasparas Kučinskas in Identity Protection, Cybersecurity

2023, November 20 · 13 min read

Surfshark®

Bundle
- Surfshark One
- Benefits

Products
- Surfshark VPN
- Surfshark Alert
- Surfshark Antivirus
- Surfshark Search
- Alternative ID
- Pricing

Other products
- Incogni

Surfshark VPN
- What is a VPN?
- VPN Features
- VPN servers
- Dedicated IP
- Reviews
- VPN download
- VPN free trial

Resources
- About us
- Media Center
- Career
- Blog
- Warrant canary

Programs
- Affiliate
- YouTube creators
- Refer a friend
- Student discount
- Graduate discount

Tools
- What is my IP
- DNS leak test
- WebRTC leak test

Support
- Help center
- Setup guides

macOS | Windows | Linux | iOS | Android | Fire TV | Chrome | Firefox | Edge

Facebook Twitter Instagram Youtube Reddit TikTok Pinterest

English

© 2023 Surfshark. All rights reserved.
Surfshark B.V., KvK number: 81967985, address: Kabelweg 57, 1014BA Amsterdam, the Netherlands, VAT number NL862287339B01

Privacy policy • Terms & conditions